UNITED STATES DISTRICT COURT

for the

Northern District of Texas

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information on Dropbox Account associated with Mark Stutheit or email mcstutheit@prodigy.net which is stored at premises owned by Dropbox

Case No. 4:16-MJ-479

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment "A"

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C.§§ 2252 and 2252A	Possession,Distribution and Receipt of Child Pornography

The application is based on these facts:

See Attached Affivadit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

LeAndrew J. Mitchell, Special Agent, HSI
Printed name and title

Sworn to before me and signed in my presence.

Date: 7/28/16

Judge's signature

City and state: Fort Worth, Texas

United States Magistrate Judge Jeffrey L. Cureton
Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, LeAndrew J. Mitchell, being duly sworn under oath, do hereby depose and state:

1. I am a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations (HSI), and I have been employed in this capacity since December 2008. I am a graduate of the Criminal Investigator Training Program and the U.S. Immigration and Customs Enforcement Special Agent Training Academy. As a result of my employment with HSI, my duties include, but are not limited to, the investigation and enforcement of Titles 8, 18, 19, 21 and 31 of the United States Code (U.S.C.). I am an "investigative or law enforcement officer of the United States" within the meaning defined in 18 U.S.C. § 2510(7), in that I am an agent of the United States authorized by law to conduct investigations of, and make arrests for, federal offenses.

2. As part of my duties as an HSI agent, I investigate criminal violations relating to child pornography, including the production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252 and 2252A. I have received training in the areas of child pornography and child exploitation, and have observed and reviewed numerous examples of child pornography, as defined in 18 U.S.C. § 2256, in all forms of media. I have been involved in numerous child pornography investigations and am familiar with the tactics used by individuals who collect and distribute child pornographic material.

3. This affidavit is being made in support of an application for a search warrant for information associated with certain accounts that is stored at premises owned, maintained, controlled, or operated by Dropbox, Incorporated,

a provider headquartered at 185 Berry Street, Suite 400, San Francisco, CA 94107. The information to be searched is further described in the following paragraphs and in Attachment A. The affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Dropbox to disclose to the Government records and other information in its possession pertaining to all subscriber(s) or customer(s) associated with or having access to the accounts referenced herein, including the contents of communications.

4. The statements in this affidavit are based in part on my investigation of this matter and on information provided by other law enforcement agents. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence of violations of 18 U.S.C. §§, 2252 and 2252A, involving the use of a computer to transport, receive, and/or possess child pornography, have been committed by Mark STUTHEIT, and that a Dropbox account further described in Attachment A contains evidence, fruits and/or instrumentalities of this crime.

5. The purpose of this application is to seize evidence, more particularly described in Attachment B, of violations of 18 U.S.C. §§ 2252(a)(4)(B) and 2252A(a)(5)(B), which make it a crime to knowingly possess and access child pornography with intent to view it; violations of 18 U.S.C. §§ 2252(a)(2) and 2252A(a)(2), which make it a crime to receive and distribute child pornography; and violations of 18 U.S.C. §§ 2252(a)(1) and

2252A(a)(1), which make it a crime to transport child pornography in or affecting interstate commerce.

DEFINITIONS

6. The following definitions apply to this affidavit and Attachment B incorporated herein:

7. "Child Pornography" includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

8. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

9. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

10. "Internet Service Providers" or "ISPs" are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail,

remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.

11. "Electronic Mail," commonly referred to as e-mail (or email), is a method of exchanging digital messages from an author to one or more recipients. Modern e-mail operates across the Internet or other computer networks. E-mail systems are based on a store-and-forward model: e-mail servers accept, forward, deliver, and store messages. Neither the users nor their computers are required to be online simultaneously; they need only connect briefly, typically to an e-mail server, for as long as it takes to send or receive messages. An Internet e-mail message generally consists of three components, the message envelope, the message header, and the message body, but may include a fourth component, an attachment. E-mail attachments can include any type of digital file. There are numerous methods of obtaining an e-mail account; some of these include e-mail accounts issued by an employer or school.

One of the most commons methods of obtaining an e-mail account is through a free web-based e-mail provider such as, MSN, Yahoo, or Gmail. Anyone that has access to the Internet can generally obtained a free web-based e-mail account.

12. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

13. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

OVERVIEW OF INVESTIGATION

14. In May 2016, an undercover police officer with the Queensland Police Service (QPS) in Brisbane, Queensland, Australia identified a profile on a website (hereinafter, "Website A"), which is known by law enforcement to be used extensively by persons interested in exchanging images depicting child pornography to meet trading partners. The owner and/or user of this profile, identified by username as "OLDMANYG," had created albums labeled "Cute butts," "Bikinis," and "9 y/o school girls." The album titled "9 y/o school girls" was password protected. The open album named "Cute butts" contained fourteen photos of prepubescent minor females wearing bathing suits; all of the photos were taken from behind, showcasing the back side of the girls' bodies.

15. Comments visible on the album made by OLDMANYG and other users indicated a sexual interest in the minors depicted in the photos. For example, on May 23, 2016, OLDMANYG posted the following comment to one of his photos, which depicted a close-up image of a minor female's buttocks in a swimming suit: "want to kiss it." On another photo depicting a minor female wearing a bathing suit, OLDMANYG posted the comment "love to look and dream." The User Information displayed on OLDMANYG's account read "Beauty is beauty, inspires feelings that not acted on. Imagination is wonderful." The account was registered on May 20, 2016.

16. The QPS undercover officer posted a message to one of OLDMANYG's photos, and OLDMANYG responded from e-mail account "fmya2x@gmail.com." OLDMANYG and the undercover officer subsequently began exchanging e-mails about the sexual exploitation of children.

In an e-mail dated May 24, 2016, OLDMANYG advised the undercover officer that he once had nude images of children, but his hard drive crashed and he would have to spend time searching his back-up to locate them.

17. The QPS obtained IP logs from Website A regarding user OLDMANYG, and determined the IP address associated with the account was 162.236.27.3. Research into this IP address revealed it is owned by Internet Service Provider AT&T, and geo-locates to the Fort Worth, Texas area. QPS investigators subsequently sent all corresponding information related to this investigation to the HSI Cyber Crimes Center (C3) for follow-up. Thereafter, HSI C3 forwarded the information to the HSI Dallas, Texas field office for investigation.

18. On May 25, 2016, HSI Special Agent Amanda Johnson sent a Department of Homeland Security summons to AT&T for the subscriber information related to IP address 162.236.27.3. On June 9, 2016, AT&T responded to the summons and provided the following subscriber information:

Name: Mark Stutheit
Address: [redacted] Sequoia Way, Saginaw, Texas 76131
Phone: [redacted]-7038
IP Start Date: May 18, 2016
IP End Date: May 22, 2016

19. On June 23, 2016, HSI agents executed a federal search warrant at [redacted] Sequoia Way, Saginaw, Texas. During the execution of the warrant, Affiant and Special Agent Johnson conducted a post-*Miranda* interview with STUTHEIT.

During this interview, STUTHEIT advised that he created a profile on Website A and uploaded albums containing images of young girls for the purpose of communicating with other users about the young girls. STUTHEIT reported his username on Website A was OLDMANYG, that he recently created the account, and that he had been chatting with numerous individuals from the website about the sexual exploitation of minors. STUTHEIT stated he began receiving e-mails with attachments containing child pornography from other users, and would download and save the material to folders on his Compaq laptop. STUTHEIT also admitted to storing child pornography in his Dropbox account. During the execution of the search warrant, Special Agent Johnson viewed numerous albums that contained child pornography in the Dropbox application on STUTHEIT's Samsung tablet. One such image, located in the "Veronica" folder, depicted a nude prepubescent minor female lying supine on a couch. The minor is using her hands to spread her genitals apart while she digitally penetrates her vagina. The focus of the image is on the minor's genitals. Computer forensics agents on-site during the warrant determined the file was created on STUTHEIT's computer on or about June 17, 2016. Special Agent Johnson has reviewed the image, and informed Affiant that it appears to depict a real minor female engaged in sexually explicit conduct.

20. Special Agent Johnson showed STUTHEIT the images from the "Veronica" folder in the Dropbox application, and STUTHEIT stated he originally received the images via e-mail at fmya2x@gmail.com and uploaded them to his Drobox account by using the Internet. STUTHEIT advised he created the Dropbox account using his current e-mail account, fmya2x@gmail.com.

21. Pursuant to the search warrant, HSI seized multiple electronic devices claimed by STUTHEIT, which were found to contain images depicting child pornography. Preliminary forensics conducted on-site during the execution of the warrant indicated STUTHEIT was in possession of hundreds of files depicting child pornography, and that STUTHEIT had used multiple devices, including, but not limited to his smartphone, laptop and tablet to transport, receive, and/or access child pornography.

22. The Samsung tablet referenced in Paragraph 19 was one of the items seized from STUTHEIT, and was subsequently submitted to the computer forensic lab at the Tarrant County District Attorney's Office in Fort Worth. Computer Forensic Examiner Huey Nguyen conducted a forensic analysis of the tablet and prepared a report. Special Agent Johnson was provided the report; and after reviewing its contents, determined the only Dropbox account used on the Samsung tablet was associated with e-mail address **mcstutheit@prodigy.net**.

23. On July 12, 2016, HSI served legal process on Dropbox for the subscriber information related to the Dropbox account associated with the e-mail account **mcstutheit@prodigy.net**. On July 25, 2016, Dropbox responded and provided records that indicate the account associated with **mcstutheit@prodigy.net** was created on June 8, 2015 by Mark STUTHEIT. The most recent IP address captured by Dropbox was 162.236.27.3, on June 11, 2016. As disclosed in Paragraph 18 of this affidavit, this IP address was captured by Website A, and later determined to be assigned to STUTHEIT's residence.

Dropbox records further indicate the account was used to add and remove files from June 8, 2015 until June 19, 2016, which was approximately three days prior to the search warrant execution at STUTHEIT's residence.

OVERVIEW OF DROPBOX

24. Dropbox is a service provider that allows its users to store and share files on Dropbox's servers. According to Dropbox's privacy policy, located at https://www.dropbox.com/privacy, Dropbox collects and stores the files a user uploads, downloads, or accesses with the Dropbox Service. The privacy policy also states that Dropbox automatically records information from a users' device, its software, and their activity using the Dropbox service. This may include the device's IP address, browser type, the web page visited prior to accessing the Dropbox website, locale preferences, device identification, and various other records. Dropbox is a free service that allows users to save files to their Dropbox account via cloud storage, which allows them to be accessed from any computer, smartphone or tablet with Internet access.

25. In general, providers like Dropbox ask each of their subscribers to provide certain personal information when registering for an account.

This information can include the subscriber's full name, physical address, telephone numbers, e-mail addresses, and/or a means and source of payment (for paying subscribers). Providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., sessions) times and durations, the types of services utilized, the status of the account

(including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, providers often maintain records of the IP address used to register the account and the IP address(es) used to access the account. Because every device that connects to the Internet must use an IP address, IP address information can help identify which computers or other devices were used to access the account.

26. Based on training and experience in child pornography investigations, Affiant is aware that cloud storage services, like Dropbox, are commonly used by individuals involved in trading child pornography. Use of services like Dropbox are often preferred by child pornography offenders because, instead of having to distribute or receive multiple e-mails containing megabytes of images and videos depicting child pornography, which could potentially be flagged by the Email Service Provider, an individual can simply forward the hyperlink to his/her cloud storage account to the intended recipient. The recipient can then view all of the file(s) associated with the Dropbox account from his/her own computer, and download any content they wish to save. Services like Dropbox are also preferred by child pornography offenders because it allows offenders to access their collection of child abuse material from multiple devices, without having to save content to either specific device. To date, Affiant has been involved in numerous investigations in which Dropbox was used to distribute, receive and store images and videos of child pornography.

CONCLUSION

27. Based on the information set forth in this affidavit, Affiant submits there is probable cause to believe that 18 U.S.C. §§ 2252 and 2252A have been violated, and that computer systems under the control of Dropbox, Incorporated contain evidence and instrumentalities of these crimes. Specifically, there is probable cause to believe that the Dropbox account associated with email account **mcstutheit@prodigy.net** will contain evidence and instrumentalities of these offenses. Affiant therefore requests that this Court issue a search warrant requiring Dropbox to produce the records outlined in Attachment A, so that agents may analyze and seize the items outlined in Attachment B.

28. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711(3) and 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that - has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(I).

29. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

LeAndrew J. Mitchell
Special Agent
Homeland Security Investigations

Subscribed and sworn to before me on July 28, 2016, at 2:35 a.m./p.m. in Fort Worth, Texas.

JEFFREY L. CURETON
United States Magistrate Judge

ATTACHMENT A
PROPERTY TO BE SEARCHED

This warrant applies to information associated with the Dropbox account that was created, utilized and/or maintained by **Mark Stutheit**, and/or associated with the e-mail address **mcstutheit@prodigy.net**, which is stored at premises owned, maintained, controlled, or operated by Dropbox, a company headquartered at 185 Berry Street, Suite 400, San Francisco, CA 94107.

ATTACHMENT B
DESCRIPTION OF ITEMS TO BE SEIZED AND SEARCHED

In order to ensure that agents search only those computer accounts and/or computer files described herein, this search warrant seeks authorization to permit employees of Dropbox Inc., to assist agents in the execution of this warrant. To further ensure that agents executing this warrant search only those accounts and/or computer files described below, the following procedures have been implemented:

1. The warrant will be presented to Dropbox, Inc., personnel by law enforcement agents. Dropbox, Inc., personnel will be directed to isolate those accounts and files described below;

2. In order to minimize any disruption of computer service to innocent third parties, the system administrator will create an exact duplicate of the accounts and files described in Attachment A, including an exact duplicate of all information stored in the computer accounts and/or files described below;

3. Dropbox, Inc., system administrator will provide the exact duplicate of the accounts and files described below and all information stored in those accounts and /or files to the Special Agent who serves this search warrant;

4. Law enforcement personnel will thereafter review the information stored in the accounts and files received from the system administrator and then identify and copy the information contained in those accounts and files which are authorized to be further copied by this search warrant;

5. Law enforcement personnel will then seal the original duplicate of the accounts and files received from the system administrator and will not further review the original duplicate absent an order of the Court.

I. Information to be disclosed by Dropbox, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of Dropbox, including any messages, records, files, logs, images, videos, or information that have been deleted but are still available to Dropbox, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Dropbox is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, e-mail addresses, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

b. All information automatically recorded by Dropbox from a user's Device, including its software and all activity using the Services, to include, but not limited to: a utilizing device's IP address, browser type, web page visited immediately prior to

connecting to the Dropbox website, all information searched for on the Dropbox website, locale preferences, identification numbers associated with connecting devices, information regarding a user's mobile carrier, and configuration information;

c. The types of service utilized by the user;

d. All records or other information stored by an individual using the account, including all files uploaded, downloaded or accessed using the Dropbox service, including all available metadata concerning these files. The contents of all folders associated with the account, including stored or preserved copies of files sent to and from the account, the source and destination addresses associated with file, and the date and time at which each file was sent;

e. All transactional information of all activity of the Dropbox accounts described above, including log files, messaging logs, records of session times and durations, dates and times of connecting, and methods of connecting: and e-mails "invites" sent or received via Dropbox, and any contact lists.

f. All records pertaining to communications between Dropbox and any person regarding the account, including contacts with support services and records of actions taken; and

g. All records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts. This includes the information listed in a. above for any person who accessed, downloaded, or uploaded from the account.

II. Information to be seized by the Government

All records or information, including the contents of any and all wire and electronic communications, attachments, stored files, print outs, and header information that contain evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. §§ 2252 and 2252A (Receipt, Possession and Distribution of Child Pornography), including, but not limited to, for each account or identifier listed on Attachment A, information pertaining to:

a. The receipt, possession, or distribution of videos, photos, or visual depictions of minors that may reside. Furthermore the receipt, possession, or distribution of personal identifying information and financial account numbers, including, but not limited to credit card verification values (CVV) and victim names, addresses, dates of birth, and financial account numbers.

b. The contents of any such communications that will assist investigators in ascertaining the nature and scope of the crimes under investigation, the true identity and or location of the subjects and their co-conspirators, the names, addresses, and locations

of victims, and any disposition of the proceeds of the crimes under investigation, including,

c. Records relating to who created, used, or communicated with the account or identifier.